UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 825 S. HILL STREET, APARTMENT 5005 LOS ANGELES, CA 90014	)	Case No. 2:22-MJ-01797

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343, 1956; 21 U.S.C. §§ 841, 846; and 31 U.S.C. § 5324.	See affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Sarah Plantz

Applicant's signature

Special Agent Sarah Plantz

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Jacqueline Chooljian, U.S. Magistrate Judge

Printed name and title

AUSA Andrew Brown, x0102, 11th Floor

ATTACHMENT A

THE PREMISES TO BE SEARCHED IS:

825 S. HILL STREET, APARTMENT 5005, LOS ANGELES, CA 90014 ("**RESIDENCE 3**"). **RESIDENCE 3** is an apartment on the northwest corner of floor 50 of 825 S. HILL STREET. The apartment complex is located on the northwest side of S. HILL STREET between 8th and 9th Streets. The main entrance to 825 S. Hill STREET is marked by a large blue sign with the name 825 SOUTH HILL printed in white letters that runs perpendicular to the street. The apartment door to **RESIDENCE 3** is clearly marked by a placard directly to the right of the door with the numbers 5005 clearly printed in white. **RESIDENCE 3** includes the assigned PARKING SPACES 387 and 122, which are located in the underground parking garage for 825 S.HILL STREET, and have the numbers "387" and "122" stenciled on them respectively in white paint, and are marked by placards that say "ASSIGNED PARKING". The premises to be searched includes vehicles parked in the assigned parking spaces.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1343 and 1956; 21 U.S.C. §§ 841 and 846; and 31 U.S.C. § 5324 (the "TARGET OFFENSES"), namely:

a. Narcotics and controlled substances, such as marijuana and THC, and related paraphernalia such as scales, pay-owe sheets, packaging material such as vape cartridges, and documents referring or relating to them, such as their manufacture or sale, or maintaining premises for the same;

b. Records referring or relating to countersurveillance of law enforcement, obstructing investigations, warning persons of law enforcement inquiries or activities such as serving subpoenas or search warrants, or hiding, altering, or destroying evidence;

c. Money counters, cash over $5,000, casino chips, prepaid cards, fungible forms of precious metals such as ingot, bullion, or coins of at least one troy ounce, and records referring or relating to the preceding items or to IRS form 8300, Currency Transaction Reports and other Bank Security Act (BSA) requirements, currency reporting requirements generally, structuring transactions to circumvent those requirements, such as instructions to keep transactions under $10,000 in cash, anti-money laundering programs and how to evade them, investigations by financial institutions and the closure or threatened closure of financial accounts, and, since 2019, records of cash payments and receipts;

d. Firearms, ammunition, and related paraphernalia such as holsters and magazines, and records referring or relating to the same;

e. Documents and records referring or relating to actual or threatened violence, such as those to enforce a criminal debt;

f. Documents and records referring or relating to COVID-relief programs such as Small Business Administration loans, the Paycheck Protection Program, Economic Injury Disaster Loans, and COVID-enhanced unemployment benefits;

g. Documents and records referring or relating to Muha Meds;

h. Mail matter and shipping packages, opened or unopened, not addressed to or from 825 S. HILL, LOS ANGELES and documents or records referring or relating to the same;

i. Personal identifying information of individuals other than those residing at 825 S. HILL, APARTMENTS 5001, 5002, and 5005, LOS ANGELES, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, PINs, credit reports, and bank or other financial institution information, and records referring or relating to such information;

j. Documents and keys relating to public storage units, rental cars, prepaid cellular telephones, safety deposit boxes, Commercial Mail Receiving Agencies, or receiving mail at someone else's address;

k. Records referring or relating to countersurveillance of law enforcement, prison, arrests, criminal investigations, criminal charges, asset forfeiture, investigations by financial

institutions, and the threatened or actual closure of accounts by financial institutions;

l. Documents and records referring or relating to the conversion of cash to financial instruments such as checks and wire transfers, and vice versa, for a percentage of the dollar value converted, or the transfer of cash abroad, such as through Hawalas or money transferring businesses, like Western Union;

m. Records relating to wealth and the movement of wealth since 2019, such as tax returns and forms, crypto-currency accounts and transfers, other digital wealth storage and transfer methods including PayPal and Venmo, money orders, brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, transactions involving prepaid cards, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $1,000;

n. Records or items containing indicia of occupancy, residency or ownership of any location or vehicle being searched, such as keys, rental agreements, leases, utility bills, identity documents, cancelled mail, and surveillance video;

o. Documents and records showing electronic and telephone contacts and numbers called or calling, such as SIM cards, address books, call histories, telephone bills, and Signal, ICQ, Telegram, and email addresses.

p. Cryptocurrency and related records and items, such as those referring or relating to public or private keys or addresses, or cryptocurrency wallets or their parts, including "recovery seeds" or "root keys" which may be used to regenerate a wallet. Seizure of the cryptocurrency and wallets will be accomplished by transferring or copying them to a public cryptocurrency address controlled by the United States, or by restoring them onto computers controlled by the United States.

q. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the TARGET OFFENSES, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the

search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team will not search for similar evidence outside the scope of the items to be seized without first obtaining authority to do so.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

8. During the execution of this search warrant, law enforcement is permitted to: (1)depress the thumb and/or fingers of ALI GARAWI, RASOOL GARAWI, or MUHAMMAD GARAWI onto the fingerprint sensor of the device(only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (d) hold the device in front of the face of ALI GARAWI, RASOOL GARAWI, and MUHAMMAD GARAWI, with their eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to

the authority conferred by this warrant, and do not apply to any other search of digital devices.

AFFIDAVIT

I, Sarah E. Plantz, being duly sworn, hereby depose and state as follows:

I. TRAINING AND EXPERIENCE

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since December 2020. I am currently assigned to the Los Angeles Field Division, White Collar Crimes Squad which is responsible for investigating financial institution fraud, including bank fraud, wire fraud, and money laundering. Since joining the FBI in 2020, I have received 22 weeks of formal training at the FBI Training Academy in Quantico, Virginia.

2. Prior to being employed by the FBI, I served as a Police Officer with the City of Charleston Police Department for seven years, and in 2018, I was selected to become a Detective in the Special Investigations Unit, specifically the Narcotics Division. In that assignment, I worked both independently, and in a squad setting, where I led and participated in numerous investigations related to crimes involving the manufacturing, distribution, and possession of illegal narcotics within the city's jurisdiction. In that capacity, I received hours of training as a Narcotics Detective, specifically training related to identifying social media platforms involved in the

distribution of narcotics, running confidential sources, and courses for undercover operations.

3. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly. This affidavit does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only. All figures, times, and calculations set forth herein are approximate.

II. OVERVIEW

4. Ali GARAWI (hereafter "A. GARAWI"), Muhammad GARAWI (hereafter "M. GARAWI") and Rasool GARAWI (hereafter "R. GARAWI") (collectively "the GARAWI BROTHERS") are engaged in the unlawful production and distribution of cannabis products without a license in the state of California.

5. In furtherance of their criminal enterprise, the GARAWI BROTHERS created multiple Limited Liability Corporations ("LLCs") to launder the proceeds of the illegal cannabis business in attempt to conceal the nature of their cash.

6. Furthermore, the GARAWI BROTHERS used these shell corporations, whose underlying business is unlawful, to apply for Economic Injury Disaster Loans (EIDL) and Paycheck Protection Program (PPP) Loans. In doing so, the GARAWI BROTHERS obtained approximately $418,133 in government funds.

III. PURPOSE OF AFFIDAVIT: SEARCH WARRANTS

7. This affidavit is made in support of an application for a warrant to search:

a. The residence of ALI GARAWI ("A. GARAWI") at 825 S. HILL, APT 5002, LOS ANGELES, CALIFORNIA 90014, including the vehicle(s) within its assigned parking spots ("RESIDENCE 1");

b. The residence of RASOOL GARAWI ("R. GARAWI") at 825 S. HILL, APT 5001, LOS ANGELES, CALIFORNIA 90014, including the vehicle(s) within its assigned parking spots ("RESIDENCE 2");

c. The residence of MUHAMMAD GARAWI ("M. GARAWI") at 825 S. HILL, APT 5005, LOS ANGELES, CALIFORNIA 90014, including the vehicle(s) within its assigned parking spots ("RESIDENCE 3"); and

d. The digital devices previously seized from M. GARAWI and R. GARAWI by the California Department of Cannabis Control (CDCC) during their execution of their search warrants in March 2021, which are stored at the IT Evidence Control Center, in Orange County, California, under CDCC case number 20-03031-CE.

for the items described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C § 1343 (wire fraud) and 1956 (money laundering), 21 U.S.C § 841 and 846 (drug trafficking), and 31 U.S.C. § 5324 (structuring) (collectively the "Target Offenses"). The residences to be searched are further described in Attachment A and are collectively referred to as the SUBJECT PREMISES. Attachments A and B are attached and incorporated.

IV. HISTORY OF INVESTIGATIONS

THE GARAWI'S UNLICENSED CANNABIS BUSINESS

7. In March of 2021, the California Department of Cannabis Control (CDCC) executed a multi-location search warrant on a large-scale unlicensed cannabis distributor and manufacturer in Los Angeles County known as "Muha Meds." During the search warrants, Agents seized approximately 986 pounds of cannabis flower, over 349,000 cannabis vape cartridges, approximately 929 pounds of edibles, and approximately 970 pounds of cannabis concentrates. The total retail value of all cannabis related items was estimated at approximately $31,147,188. Additionally, $185,273 of cash was seized from the operation and approximately $200,000 was seized from various bank accounts titled to Muha Enterprises.

GARAWI'S BOX AT U.S. PRIVATE VAULTS

8. In March 2021, the United States Postal Inspection Service (USPIS), Federal Bureau of Investigation (FBI) and Drug Enforcement Administration (DEA) executed federal search and seizure warrants at U.S. Private Vaults ("USPV")[1], a private anonymous safe deposit box company. The warrant authorized, among other things, seizing the nests of safety deposit boxes at USPV as evidence and instrumentalities of the offenses committed by USPV. An inventory search was conducted on all the boxes at USPV, including BOX 1805, belonging to A. GARAWI. The box

[1] From speaking with the case agents from the United States Postal Inspector's Service ("USPIS") and Drug Enforcement Administration ("DEA") and the FBI, and reading their reports, I know that U.S. Private Vaults is a business in a strip mall that rented safety deposit boxes anonymously. It was owned and managed by criminals who engaged in money laundering, drug trafficking, and structuring, among other offenses. Its business model was designed to appeal to criminals for customers. It charged many times what banks do for similar safety deposit box rentals, but staff conducted counter-surveillance for customers, alerted them to law enforcement investigations, and structured transactions for them to avoid filing currency reports--in addition to providing them a place to store criminal proceeds anonymously. USPV also laundered for its customers cash that was purported to be drug proceeds by converting it into precious metals or wire transfers. The great majority of USPV customers paid cash to rent their safety deposit boxes, at least some of which USPV then deposited into their own bank account, which it used to pay its operating expenses. By using its customers' criminal proceeds to maintain its own anonymous facility for the storage of criminal proceeds, USPV engaged in money laundering. I know from reading the indictment that on March 9, 2021, USPV was indicted by a federal grand jury for conspiring with its customers and others to launder money, distribute drugs, and structure financial transactions to avoid currency reporting requirements. I am also aware that in In March 2022, U.S. Private Vaults, Inc. pleaded guilty to a conspiracy with its customers to launder drug proceeds.

contained $628,740 in U.S. Currency, as well as paperwork which identified A. GARAWI as the box holder. The cash was presented to a narcotics detecting canine at the scene. The canine gave a positive indication for the presence of narcotics.

9. On December 15, 2021, I reviewed a declaration by Officer Angel Bran, who is a canine Officer for Chino Police Department. Officer Bran stated in his report that on March 23, 2021 at 2019 hours, while the search warrant for USPV was being executed, federal agents presented the cash from BOX 1805 (A. GARAWI'S box) to his drug detecting Police Service Dog, "CYRA." Officer Bran stated that "CYRA" alerted to the presence of the odor of illegal narcotics emitting from the contents of BOX 1805.

10. Based on Officer Bran's declaration, I know that Cyra has received over 240 hours of instruction in the detection of the odor of illegal drugs. Additionally, I learned that Officer Bran and Cyra passed a certification test in the detection of the odor of illegal drugs. During the course, Officer Bran personally observed Cyra alert to the presence of the odor of illegal drugs and is familiar with Cyra's behavior when she detects the odor of illegal drugs. Additionally, Officer Bran advised investigators in this case that as a part of their regular training and yearly certification process, Cyra is subjected to blind, controlled tests in which different types

of illegal drugs are hidden in different places in a large training facility. Their handlers do not know where the drugs are. If the canines alert to an area that does not contain drugs, or fails to locate any of the drugs, the canine would fail and not be certified.

11. In March 2022, U.S. Magistrate Judge Alexander Mackinnon authorized a warrant to search A. GARAWI'S safety deposit box. Additionally, the FBI obtained a warrant for the cell-site information, GPS information, and information from cell-site simulator on GARAWI's telephone (2:22-MJ-01231) (the "SUBJECT TELEPHONE"). Results of that warrant have placed A. GARAWI at RESIDENCE 1, as described more fully below.

V. PROBABLE CAUSE STATEMENT

INDIVIDUALS AND ENTITIES INVOLVED

12. A. GARAWI, R.GARAWI, and M.GARAWI are brothers who are engaged in the unlawful manufacturing and distribution of cannabis products. According to the CDCC, their cannabis related activities are not licensed by the State of California. In furtherance of this enterprise, the GARAWI brothers have created a number of LLC's to launder the proceeds of their cannabis business and conceal the true nature of the money. Based on a search of the California Secretary of State, those entities include:

a. Golden Exclusive Properties Incorporated, "a wholesale goods business"[2] , which lists A. GARAWI as the Chief Executive Officer (CEO), and M. GARAWI as the Secretary of the corporation.

b. Habibi Enterprises LLC, "a wholesale merchandise" business, which lists A. GARAWI as the CEO of the company.

c. Muha Enterprises LLC, "a wholesale merchandise", which lists M. GARAWI as the CEO of the company.

d. 7K Digital LLC, "a management consultant and web developing company", which lists R. GARAWI as the CEO of the company.

13. Golden Exclusive Properties Inc., Habibi Enterprises LLC, and Muha Enterprises LLC, all used the shared address of 8337 Lexington Road, Downey, California 90241.[3]

GARAWI BROTHERS INVOLVEMENT IN CANNABIS/MARIJUANA

14. As described above, in March 2021, the CDCC executed multi-location search warrants targeting the GARAWI BROTHERS' unlicensed and illegal cannabis business (Muha Meds). As a

[2] This business description "wholesale goods," was listed on California Secretary of State forms and is, we believe, intentionally vague, so as to conceal the true nature of the business, which is the unlawful manufacture and distribution of whole sale marijuana and cannabis products.

[3] Based on open source research and law enforcement databases, we believe this address belongs to the parents of the GARAWI BROTHERS, and is a "permanent address" used by them to receive mail, but not an address used for business operations or residency.

result of those search warrants, the CDCC seized millions of dollars' worth of contraband and clear evidence of their participation in an illegal enterprise.

15. After reviewing the CDCC's Search Warrant Affidavits regarding the Muha Meds cannabis and marijuana company, I learned the following facts:

a. The GARAWI BROTHERS were all involved in the unlicensed cannabis business titled Muha Meds as further described below.

b. The Muha Meds merchandise website (muhameds.com) was created by R. GARAWI and began actively advertising in December of 2019.

c. The phone number listed for the website (muhameds.com) was registered to A. GARAWI.

d. True Terpenes, a cannabis oil company, observed on the Muha Meds website and Instagram page, provided an email address of Muhammadgarawi@gmail.com which I believe belongs to M. GARAWI.

e. Muha Enterprises LLC has an account with Think 20 labs, a laboratory involved in testing cannabis, located in Irvine, California. Think 20 labs was advertised on the Muha Meds website and Instagram page.

f. A. GARAWI and M. GARAWI were both observed at the

search warrant locations on multiple days that the CDCC conducted surveillance, prior to the CDCC executing the search warrant.

g. M. GARAWI and R. GARAWI were present at Muha Meds when the CDCC warrant was served.

16. That the GARAWI BROTHERS' various corporations are fronts for their cannabis business is further supported by the following:

a. According to an article[4] in "Ganjapreneaur", a cannabis-industry trade publication, A. GARAWI is the CEO of Muha Meds, "A self-described street cannabis brand that is best known for the unregulated sale of THC-rich vape cartridges." The article provided an Instagram link to a web page with numerous photos of A. GARAWI, which match the California Department of Motor Vehicles (DMV) photograph of A. GARAWI.

b. Furthermore, Agents learned that Muha Meds also operates as Habibi Enterprises LLC, according to an article located in Magcloud.com[5].

[4] "Widely Counterfeited Muha Meds Vape Brand Now Licensed In Michigan" by Graham Abbott, October 20, 2021; Ganjapreneur,https://www.ganjapreneur.com/widely-counterfeited-muha-meds-vape-brand-now-licensed-in-michigan/

[5] MagCloud, Habibi Enterprises LLC (Muhameds), November 30, 2020, https://www.magcloud.com/user/muhameds

LOANS OBTAINED FRAUDULENTLY BY GARAWI BROTHERS

17. During the COVID-19 pandemic, the Small Business Administration (SBA) provided Economic Injury Disaster Loans (EIDL) for businesses to help overcome the effects of the pandemic by providing working capital to meet operating expenses. The EIDL funds were to be used for payroll, rent/mortgage, utilities, payments due on federal debts, and payments for business non-federal debts incurred at any time. The SBA listed numerous business entities that were eligible to receive EIDL funds and listed a numerous business entities that were ineligible to receive funds. The ineligible entities included the following:

a. "Engaged in any illegal activities at the federal, state or local level (including sale of marijuana/cannabis)" (About Covid-19 EIDL)

18. The purpose of the Paycheck Protection Program (PPP) was to provide a direct incentive for small businesses to keep their workers on payroll. The PPP loans were to be used for payroll costs, including benefits, mortgage interest, rent, utilities, worker protection costs, uninsured property damage costs caused by looting or vandalism during 2020, and certain supplier costs and expenses. The SBA also lists numerous entities that may qualify for PPP loans, however on the application for the PPP loans, the signer of the loan is to

agree to the following:

a. "The Applicant is not engaged in any activity that is illegal under federal, state or local law."

19. On July 12, 2020 Golden Exclusive Properties Inc., applied for a $150,000 EIDL loan. The loan was disbursed into Citi Bank account ending in 0097, titled to Golden Exclusive Properties with signer A. GARAWI, on August 6, 2020. Furthermore, the application stated that Golden Exclusive Properties Inc. had two employees as of January 31, 2020.

20. Muha Enterprises LLC, applied for a $150,000 loan on July 08, 2020. The loan was disbursed into US Bank account ending in 4188, titled to Muha Enterprises with signer M. GARAWI, on July 14, 2020. The application stated that Muha Enterprises LLC had two employees as of January 31, 2020.

21. Habibi Enterprises LLC, applied for a $20,833 PPP loan On June 29, 2020. The application was signed and submitted by A.GARAWI, who claimed 100 percent ownership of the business. The loan was disbursed into Chase Bank account 2872 on June 29, 2020.

22. 7K Digital LLC, applied for a $97,200 loan on July 8, 2020. The loan was disbursed into Citi Bank account ending in 9489, titled to Art of Marketing with signer R. GARAWI, on August 5, 2020.

23. According to the Employment Development Department for

the State of California, there were no employment records associated with Golden Exclusive Properties, Habibi Enterprises, or A. GARAWI within the first quarter of 2019 through the fourth quarter of 2021. Additionally, there is no physical location or a "brick and mortar" store front for any of these businesses.

24. Based on the CDCC warrants, the open source articles cited, and the presence of over $600,000 in cash located at an anonymous safe deposit company, I believe all business entities created and controlled by the GARAWI BROTHERS are engaged in the unlawful sale of cannabis and/or the laundering of criminal proceeds. As such, the businesses were ineligible for government loans. Moreover, the apparent falsehood on the application regarding the number of employees suggests additional fraud in obtaining these loans.

GARAWI BROTHERS LAUNDERING MONEY WITHIN LLC's

25. In December 2021, I reviewed bank records for the following accounts associated with the GARAWI BROTHERS companies:

a. Citi Bank Account 0097, titled to Golden Exclusive Properties, with signer A. GARAWI ("Account 1").

b. Citi Bank Account 9489, titled to Art of Marketing LLC, with signer R. GARAWI ("Account 2").

c. US Bank Account 4188, titled to Muha Enterprises LLC, with signer M. GARAWI ("Acccount 3").

26. In reviewing these accounts, I observed a pattern of frequent fund transfers among these accounts, with no apparent business purpose. For example:

a. In Citi Bank account 0097, titled to Golden Exclusive Properties, I observed three deposits from Habibi Enterprises LLC, totaling approximately $67,644. I observed nine deposits from A. GARAWI's personal account, totaling approximately $46,040, and I observed two transfers to Citi Bank account 9489, titled to Art of Marketing LLC, totaling approximately $35,000.

b. In Citi Bank account 9489, titled to Art of Marketing LLC, I observed twenty-three deposits from R. GARAWI, mostly including deposits from his Apple Cash account, totaling approximately $61,353.

27. Based on my training and experience, I am aware that criminals who seek to disguise or conceal the origins of their money often engage in "layering." This is the process of moving money in and out of various bank accounts, with no business purpose, in order to launder the money, conceal its origins, and frustrate law enforcement in any attempt to trace the funds to their illegal source. In reviewing the listed bank accounts, all held and controlled by one or more of the GARAWI BROTHERS, I

observed regular movement of funds between the GARAWI BROTHERS accounts, with no apparent purpose.

28. Additionally, by depositing fraudulently obtained PPP and EIDL loan money into these accounts, the GARAWI BROTHERS have co-mingled criminal proceeds (fraud) with criminal proceeds (marijuana) and any other legally obtained money is thereby also tainted.

DIGITAL DEVICES PREVIOUSLY SEIZED FROM GARAWI BROTHERS

26. On March 9, 2021, CDCC executed a multi-location search warrant on Muha-Meds. During this search warrant, the CDCC seized numerous digital devices from the individual locations as well as the two brothers on scene at the time of the search warrant, R. GARAWI and M. GARAWI. The passwords to the devices were requested from R. GARAWI and M. GARAWI, but they declined to provide them. The CDCC attempted to gain access to the digital devices but was unsuccessful, in part due to lack of resources. It is believed that the FBI's Computer Analysis Response Team (CART) is better equipped to gain access to the devices based on the resources and personnel available.

27. The devices are currently in the possession of the CDCC, located at their IT Evidence Control Center, in Orange County, California. The Digital Devices are labeled under the CDCC case number 20-03031-CE.

VI. REASON TO BELIEVE THE INDIVIDUALS LIVE AT THE TARGET LOCATIONS

28. Pursuant to Judge MacKinnon's GPS warrant, I started to receive the GPS coordinates for the SUBJECT TELEPHONE from the telephone service provider. Between April 1, 2022 and April 6, 2022, the SUBJECT TELEPHONE was located in or around Royal Oak, Michigan, a suburb of Detroit. On April 6, 2022, the SUBJECT TELEPHONE arrived back into Los Angeles. It was observed that on April 6, 2022 at approximately 8:45 PM, the SUBJECT telephone was in the area of 8th Street between S. Hill Street and S. Olive Street, located in downtown Los Angeles. The ping provided an approximate radius of 182 meters. This distance would encompass the area immediately surrounding the ping, which would include the 825 S. HILL Apartments located less than .1 miles from where the ping registered.

29. Throughout April 2022, I observed that the SUBJECT TELEPHONE pinged in the immediate area surrounding 825 S. HILL Apartments for long periods of time, especially during the night time hours, for consecutive days.

30. In December 2021, I reviewed bank records for ACCOUNT 1 (held by A. GARAWI) and I observed consecutive monthly payments being withdrawn to "YSI 825 SOUTH HILL", which appeared to be on schedule with a rent payment. I also reviewed bank records for ACCOUNT 2 (Held by R. GARAWI) and I observed

similar consecutive monthly payments being withdrawn to "YSI 825 SOUTH HILL", which are believed to be monthly rent payments.

31. In April 2022, I reviewed lease records from 825 S. HILL Apartments stating that A.GARAWI was the lease holder for APARTMENT NUMBER 5002, R. GARAWI was the lease holder for APARTMENT 5001, and M. GARAWI was the lease holder for APARTMENT 5005, all located within 825 S. HILL APARTMENTS.

32. According to the Property Manager of 825 S. HILL Apartments, RESIDENCE 1, RESIDENCE 2, and RESIDENCE 3 each have assigned parking spots within the parking garage located below the apartment building. RESIDENCE 1 is assigned PARKING SPOT 203 and PARKING SPOT. RESIDENCE 2 is assigned PARKING SPOT 504 and PARKING SPOT 509. RESIDENCE 3 is assigned PARKING SPOT 387 and 122.

33. Furthermore, The GARAWI BROTHERS have been observed driving a large variety of different vehicles in and out of the parking garage. The Property Manager provided a list of vehicles that have previously been registered with the apartment building but advised that it is not current due to the vehicles consistently changing. The list included vehicles such as Range Rovers, Mercedes, Lamborghinis, Dodge RAM, and Tesla.

34. On April 29, 2022 Agents observed the following vehicles within the assigned parking spots:

a. PARKING SPOT 504 was vacant.

b. PARKING SPOT 509 was vacant.

c. PARKING SPOT 203 had a white BMW bearing CA Tags: 8RXU061 registered to Golden Exclusive Properties with address 825 S. HILL APARTMENT 5002, LOS ANGELES, CA 90014.

d. PARKING SPOT 208 was vacant.

e. PARKING SPOT 387 was vacant.

f. PARKING SPOT 122 had a grey BMW bearing CA Temp Tags:BG27A25, registered to Pablo Ochoa, with address 12409 Parrot Ave, Downey, CA 90242.

35. In my training and experience, I know, it is common for criminals who are fearful of having their homes searched by law enforcement to manipulate their address information so that public records indicate they live at one location when in fact they reside at a different one. I also know that it is common for criminals to consistently change vehicles in efforts to be less recognizable to law enforcement.

VII. TRAINING AND EXPERIENCE REGARDING THE SUBJECT OFFENSES

36. Based on my training and experience, and based on my consultation with other law enforcement officers, I know that:

a. Individuals involved in drug trafficking, money laundering, fraud, and structuring schemes usually keep evidence of their schemes, such as pay-owe sheets, contact

information for their co-conspirators, suppliers and customers, and records documenting the movement of criminal proceeds.

b. Individuals who launder money, structure cash, or commit bank fraud also keep ATM receipts, deposit slips, money order stubs and other evidence of financial instruments and transactions, to keep track of all the deposits and other times, keep this type of evidence at home or on their person out of carless behavior.

c. Individuals who structure cash, avoid taxes or avoid paying restitution, would often keep true records of their deposits at places they can feel safe, like their homes.

d. These individuals often use the proceeds of their crimes to purchase expensive items, or store the proceeds in the form of cash to make it more difficult to trace. Many also use their illicit cash to acquire other means of storing value, such as gold bullion or coins, prepaid cards, casino chips, and increasingly cryptocurrency.

e. Individuals involved in such offenses need to communicate with their co-conspirators about their criminal activity. There are usually records of those communications in their electronic devices, such as cellular telephones.

f. Typically, they maintain the evidence where it is

close at hand and safe, such as in their residences, vehicles, and digital devices, which are also commonly stored in their residences and vehicles. Such individuals commonly use digital devices to communicate with their fellow participants by phone, email and text message. I know that individual who commit crimes with the aid of electronic devices do not readily discard them, as computers, tablets and cell phones are expensive items that are typically used for years before being upgraded or discarded. Computers, tablets, and cell phones can be used to communicate between co-conspirators and may contain information relating to the crime under investigation.

g. I know from training and experience that individuals involved in fraud keep the most damaging evidence and/or proceeds of the scheme at their residences, vehicles, garages and to help conceal the fraud from their fellow coworkers who may have access to such documents at the workplace. More sophisticated or cagey criminals may rent public storage units or safety deposit boxes, especially when storing valuables such as cash, to further distance themselves from incriminating evidence.

h. I know from training and experience that individuals who are evading paying taxes would keep funds outside of traditional banking and would rather keep

valuables and cash at places out of the FTB or IRS' reach such as USPV, or at their homes.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

37. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remains on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining

records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, email, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

38. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence reference above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are no commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size word documents, or 614 photos with an average size of 1.5MB.

39. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of

publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time, (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. The passcodes for the devices likely found in the search are unknown.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that

appears to have a biometric sensor and falls within the scope of the warrant: 1. Depress the thumb and or fingers of A. GARAWI, R.GARAWI, and M.GARAWI on the device(s) and 2. Hold the device(s) in front of A.GARAWI, R. GARAWI, and M. GARAWI'S face with their eyes open to activate the facial-, iris-, and/or retina- recognition feature.

40. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

IV. CONCLUSION

36. For the reasons stated above, there is probable cause to believe that evidence and proceeds of the TARGET OFFENSES, as described more particularly in Attachment B, are in the SUBJECT PREMISES.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of May, 2022.

_____
UNITED STATES MAGISTRAGE JUDGE